<http://thehackernews.com/2013/03/reserve-bank-of-australia-hacked-by.html>

Summary:

The Reserve Bank of Australia (RBA) was hacked by hackers by sending the RBA staffs emails that linked to a zip file that contained a Trojan in order to infiltrated RBA’s networks and stole information. Investigation showed that some computers compromised by malicious software and even the heads of department received the malicious emails.

Six users clicked on the link contained in the mail but those affected computers did not have local administrator rights, so the virus could not spread. The investigation showed that the anti-virus program does not detect the attack when the email received. The RBA will continue doing the investigations and monitor cyber incidents.

Analysis

First, this attack can detected earlier if the staff was trained be more security dealing with incoming information. Suspicious email or link should not be open if the sender or content are not in trust list, or should report to IT security manager.

Secondly, this attack indicates the firewall or monitor system in RBA is weak. If it can detect and block the access via the link in the email, the Trojan program will not be able to downloaded and executed. Furthermore, this Trojan program is zipped, indicate RBA should build up a firewall to check the incoming zipped file to make sure any executable program in it is safe, or at least give warning to the user.

The good news is that, the six malicious computers have no local administrative right so that the Trojan cannot spread in the bank internal system. If the malicious computer has this right, it will be able to access or steal customer information, bank account, etc.